

UNITED STATES DISTRICT COURT

Northern District of California

San Francisco Division

In the Matter of the Application of

No. C 13-80125 CRB (LB)

O2CNI CO., LTD.,

For an Order to Conduct Discovery for Use in
a Foreign Legal Proceeding pursuant to 28
U.S.C. § 1782.**ORDER DENYING PETITIONER'S
SECTION 1782 APPLICATION FOR
DISCOVERY TO PROVIDE TO
KOREAN POLICE IN THEIR
CRIMINAL INVESTIGATION OF
RESPONDENTS AND OTHERS**

[Re: ECF No. 1]

INTRODUCTION

Petitioner O2CNI is a Korean company that contracted with a Korean subsidiary of Symantec Corporation, a United States corporation, to provide remote technical support via Korean call centers to Korean and Japanese end users of Symantec's anti-virus and security product Norton Utilities. Symantec¹ ended that relationship, and then its subsidiary Symantec Korea hired five former O2CNI employees and started providing the same technical support via its own Korean call center. Shin Decl., ECF No. 5, ¶¶ 9-20.² Symantec Korea apparently pushed O2CNI out of the market, and

¹ Where appropriate, the court refers to Symantec Corporation and its various subsidiaries generically as "Symantec." When specificity is needed, the court refers to the particular entity discussed.

² Citations are to the electronic case file ("ECF") with pin cites to the electronically-generated page numbers at the top of the page.

O2CNI attributes that success to the former O2CNI employees' disclosure of O2CNI's trade secrets to Symantec Corporation and its employees, including Steven Owyang. *Id.* ¶¶ 15-24.

In June 2013, O2CNI filed an application under 28 U.S.C. § 1782 to obtain discovery in the United States from Symantec Corporation and Mr. Owyang (collectively, "Respondents") to give to Korean authorities to use in their criminal investigation into whether they should charge Symantec, Mr. Owyang and his supervisor Kevin Chapman (both of whom are Symantec employees in Mountain View, California), and the five former O2CNI employees with the criminal theft of O2CNI's trade secrets. *See* Application, ECF No. 1³; Shin Decl., ECF No. 5, ¶ 29; Shin Decl., Ex. C, ECF No. 5-2 at 7 (complaint lists Mr. Owyang and Mr. Chapman as criminal suspects). O2CNI initiated the Korean investigation by a request to Korean police in December 2011 and renewed the request in a complaint in late 2012. Shin Decl., ECF No. 5, ¶¶ 24, 29.

The alleged trade secrets are (1) a proprietary communications network that allowed Japanese customers to be billed at a lower Korean rate and (2) a modified knowledge base tailored to Japanese customers. *Id.* ¶ 11. The nexus to the United States is that in the year and a half before they left O2NCI, the former O2CNI employees had "unusually frequent" email exchanges with Mr. Owyang and Mr. Chapman. *Id.* ¶¶ 17-18. Some O2CNI employees tried to destroy their emails and computer files before they left O2CNI, but O2CNI recovered emails that allegedly suggest that the former employees disclosed confidential trade secrets to Mr. Owyang, Mr. Chapman, and other Symantec employees. *Id.*

Under 28 U.S.C. § 1782(a), a court has discretion to grant an "interested person[']s" application for discovery for use in foreign proceedings, "including criminal investigations before formal investigation." O2CNI is an alleged victim and an "interested person." The issue is, on this record and in the exercise of the court's discretion, should the court allow O2CNI to obtain discovery from

³ Originally O2CNI also sought discovery to use in anticipated civil litigation in Japan, but the court denied that request without prejudice as premature, *see* 8/15/13 Order, ECF No. 41 at 15, and O2CNI does not challenge that determination, *see* Motion, ECF No. 45 at 7 n.1. It challenges only the court's previous denial of criminal discovery as "not appropriate on this record." 8/15/13 Order, ECF No. 41 at 15. The parties supplemented their previous filings, and the district court sent the matter back. *See* 10/8/13 Order, ECF No. 50 (referencing the Shin Declaration at ECF No. 28).

Symantec Corporation and Mr. Owyang here to give to the Korean prosecutors who are investigating them in Korea (at O2CNI's instigation) for alleged criminal theft of trade secrets. On this record, the court exercises its discretion and **DENIES** O2CNI's application to obtain discovery from Symantec Corporation and Mr. Owyang.

STATEMENT⁴

I. O2CNI'S AND SYMANTEC'S BUSINESS RELATIONSHIP

O2CNI (formerly PC Doctor) was one of the first providers of remote technical support services, which involve trouble shooting technical problems with a customer's computer remotely. Shin Decl., ECF No. 5, ¶ 5; Chapman Decl., Ex. A, ECF No. 21. In 2005, Symantec Corporation approached O2CNI to provide technical supports to end users of Norton Utilities, and thereafter, O2CNI contracted with Symantec's subsidiaries to provide call-center services to Norton users in Japan and Korea via its call center in Korea. Shin Decl., ECF No. 5, ¶¶ 9-12. It used a proprietary communications network that lowers fees to local Korean rates, and it used a modified knowledge base tailored to Japanese customers. *Id.* ¶ 11. These, O2CNI claims, are trade secrets. *Id.*

Between October and December 2011, five key O2CNI employees resigned and then were hired immediately by Symantec Korea. *Id.* ¶¶ 14-15. Symantec Korea assured O2CNI that the former O2CNI employees' duties at Symantec Korea were unrelated to their previous duties at O2CNI, but O2CNI learned that its former employees manage a call center in Korea that provides remote technical support that competes directly with O2CNI. *Id.* ¶¶ 19-20. Also, in the year and a half before they left O2CNI, the five employees emailed in an "unusually frequent" way with Symantec Corporation employee Steven Owyang and his supervisor Kevin Chapman without copying their O2CNI superiors (as O2CNI policies required). *Id.* ¶ 17. Some of the former O2CNI employees

⁴ The court's August 15, 2013 order recites the facts too, *see* 8/15/13 Order, ECF No. 41 at 1-7, and this order incorporates that recitation by this reference. *See also Matter of Application of O2CNI Co., Ltd.*, C13-80125 CRB (LB), 2013 WL 4442288 (N.D. Cal. Aug. 15, 2013). Because that order involved a substantial discussion about whether discovery was appropriate now for an anticipated (and possibly hypothetical) civil litigation that is not an issue for this order, this section sets forth abbreviated facts relevant to what remains at issue: O2CNI's request for discovery in aid of a Korean criminal investigation into Symantec.

1 tried to destroy their computer and email files, but O2CNI recovered emails suggesting that some or
2 all of them disclosed confidential O2CNI trade secrets to Symantec Corporation's employees
3 (including Mr. Owyang and Mr. Chapman) while the former O2CNI employees were still working
4 for O2CNI. Shin Decl., ECF No. 5 at 18.

5 As to the alleged trade secrets, according to Symantec, its agreements with O2CNI provided that
6 Symantec – and not its vendor O2CNI – owned all information and data relating to Symantec
7 products and services, support for those products and services, and Symantec customers. Chapman
8 Decl., ECF No. 21, ¶¶ 4, 7 & Exs. A-C (the agreements).

9 On July 27, 2012, O2CNI learned that its contract with Symantec Japan would not be renewed
10 upon its expiration on August 31, 2012. Shin Decl., ECF No. 5, ¶¶ 19-20. After the contract
11 expired, Symantec Korea began providing the same remote technical support services to Japanese
12 end users from its own call center in Korea, which was being managed by the O2CNI former
13 employees. *Id.* ¶ 20. O2CNI then was informed that effective December 31, 2012, all other
14 contracts related to Japan also would be terminated. *Id.* ¶ 21. Since then, O2CNI completely lost its
15 market share in Japan. *Id.* ¶ 22.

16 Symantec previously had been providing its own remote technical support in countries other than
17 Japan and Korea since 2009, but those services “had sluggish sales and were not commercially
18 viable until 2011-2012 – the very period when O2CNI believes Symantec was conspiring” with
19 O2CNI's former employees to steal trade secrets – and then Symantec's services “suddenly showed
20 dramatic improvements.” *Id.* ¶ 23. It took O2CNI nine years to build its proprietary knowledge
21 base and communications network that enabled it to be the market leader in remote technical support
22 services. Memo., ECF No. 2 at 11 (does not cite supporting facts). Symantec overtook O2CNI in
23 less than a year after it hired O2CNI's former employees, and O2CNI believes Symantec could not
24 have developed a profitable remote support service so rapidly unless it and its employees Mr.
25 Owyang and Mr. Chapman wrongfully acquired O2CNI's trade secrets and intellectual property
26 from O2CNI's former employees. *Id.*

II. THE KOREAN CRIMINAL INVESTIGATION

A. O2CNI's Role In The Korean Criminal Investigation

O2CNI submitted a request for a criminal investigation to the Korean National Intelligence Service ("NIS") in December 2011, alleging that its five former employees illegally disclosed its trade secrets to Symantec. *Id.* ¶¶ 24 & Ex. A; Hwang Decl., ECF No. 20-3 ¶ 2. This request apparently initiated the Korean investigation. The request (1) noted O2CNI's "huge contributions to Korea's advancement as an IT pioneer," (2) pointed to O2CNI's services to Japanese customers and "technological protection measures" designed "to fend off low-priced offensives from emerging countries such as China and guard against potential losses on the corporate and national levels in the form of technology and operational know-how leaks," (3) noted Symantec's demands on O2CNI for cost reduction to maximize Symantec's profits, (4) identified two of the former employees who refused to sign non-compete and confidentiality agreements that prevented them from working in the same industry, (5) identified the former employees who went to Symantec, and (6) asked for help to "prevent the leak of precious first-in-Asia assets belonging to O2CNI as well as Korea" Shin Decl., Ex. A, ECF No. 5 at 9-50. The request then described O2CNI and its technology and references evidence obtained from its server and information about the relationship with Symantec. *Id.* at 14-50.⁵

The NIS conducted a preliminary review and turned the matter over to the Gyeonggi Provincial Police Agency, which initiated a criminal investigation in February/March 2012. Shin Decl., ECF No. 5 ¶ 25; Hwang Decl., ECF No. 20-3 ¶ 2. "At various times during the investigation, Korean authorities requested O2CNI's assistance in collecting evidence in aid of the investigation," and "O2CNI has cooperated fully, providing witness testimony and turning over the documents that it has been able to locate as a result of its own efforts." Shin Decl., ECF No. 5, ¶ 26.

"In October and November 2012, in support of the Korean Criminal Proceedings, O2CNI

⁵ This document, which is translated from Korean, *see* Shin Decl., ECF No. 5, ¶ 24, references attachments and lists "Evidence on Access to Internal Servers," but does not appear to explain the alleged transmission of the trade secrets by email or any deletion issues, *see id.*, Ex. A, ECF No. 5 at 9-50.

submitted a complaint, request for punishment, and concurring opinion, alleging and providing further evidence that the Former Employees, Symantec and Symantec employees Owyang and Chapman violated the Korean Unfair Competition Prevention and Trade Secret Protection Act and wrongfully acquired, used, and disclosed O2CNI's trade secrets." *Id.* ¶ 29.

The Request for Punishment (1) is signed by O2CNI's Vice President, (2) identifies the "[n]eed to punish suspects strictly," (3) states that "severe criminal penalties should be [i]mposed on the suspects," (4) notes that "[d]ue to such a criminal activity, the technology developed by a Korean company is in danger of being fully transferred to a foreign company," and (5) projects that "[t]he expected damages to be incurred by Korean companies is at least hundred billion won . . . and reduction in employment is expected as a result." *Id.*, Ex. B, ECF No. 5-1 at 7 (underlining in original).

The complaint (1) is signed and submitted by O2CNI's lawyers in Korea, (2) lists the criminal suspects as Mr. Owyang, Mr. Chapman, the five former O2CNI employees, Symantec Corporation, Symantec Asia Pacific, and Symantec Korea, and (3) identifies Mr. Chapman as the Vice President, and Mr. Owyang as a director, of the NortonLive Consumer Service Team. *Id.*, Ex. C, ECF No. 5-2 at 1-10. The concurring opinion is signed by O2CNI's lawyers in Korea and alleges that Mr. Owyang instructed two former O2CNI employees "to leak the classified business information which belonged to [O2CNI]" *Id.*, Ex. D, ECF No. 5-2 at 29-42 (describes working on PCs with external hard drives, backing up data, and not leaving traces on the computers).

Under Korean law, the trade secrets crimes alleged by O2CNI are punishable by up to ten years' imprisonment and a fine. Son Decl., ECF No. 4, ¶ 3.

B. The Korean Police's Investigative Activities

On March 15, 2012, Korean authorities executed search warrants in Korea against the former employees and at Symantec Korea at its office in Seoul. Shin Decl., ECF No. 5, ¶ 27; Hwang Decl., ECF No. 20-3, ¶ 3. According to O2CNI's CEO, he "understand[s] that . . . Korean authorities . . . recovered significant evidence of the wrongdoing of the accused." Shin Decl., ECF No. 5, ¶ 27.

According to one of Symantec's attorneys, the authorities seized the personal computers, storage media, and the work and personal email accounts of O2CNI's former employees at their offices and

1 residences, and they also seized extensive computer media and documents from Symantec's Korea
 2 office. Hwang Decl., ECF No. 2-3, ¶ 3. The authorities have questioned the O2CNI former (and
 3 now Symantec) employees numerous times. *Id.* Those employees and a Symantec Korea
 4 representative submitted to those sessions voluntarily. *Id.* ¶¶ 3, 8. The interviews were voluntary
 5 because (according to Symantec), at the pre-indictment stage, the Korean authorities cannot compel
 6 criminal suspects to submit to an interrogation unless – upon a showing of a risk of destruction of
 7 evidence or the evidence becoming unavailable – a court issues an order. *Id.* ¶ 6 (citing Article 184
 8 of the Criminal Procedure Act). Symantec cooperated not only by having the five former O2CNI
 9 employees submit to “extensive police and prosecutorial interviews” but also by “producing
 10 voluminous amounts of documents.” Chapman Decl., ECF No. 21, ¶ 9.

11 The Korean police apparently sent formal “Requests to Appear” to Mr. Owyang, Mr. Chapman,
 12 and the CEOs of Symantec Corporation, Symantec Japan, and Symantec Asia Pacific. Park Reply
 13 Decl., ECF No. 31, ¶ 3. The basis for this knowledge is that a Korean police inspector told O2CNI's
 14 Vice President that on three occasions, he faxed formal requests to appear to the CEO of Symantec
 15 Corporation, Mr. Owyang, and Mr. Chapman, and he received delivery confirmations for his faxes.
 16 *Id.*, ¶¶ 3-4) (police inspector said that he could not provide the requests to the Vice President
 17 because they were confidential investigatory documents of the Korean police). According to
 18 O2CNI's lawyer, the Korean police told O2CNI that despite these attempts, they have been unable
 19 to (a) collect any documents from Symantec Corporation that are stored or held outside Korea, or (b)
 20 interview or collect documents from Mr. Owyang or Mr. Chapman because they are outside Korea.
 21 Shin Declaration, ECF No. 5 ¶ 28. The Korean police requested that they come to Korea voluntarily
 22 to be interviewed, but they declined. Hwang Decl., ECF No. 20-3 ¶ 8. According to Symantec, not
 23 only did it produce voluminous documents voluntarily to the Korean police but also, “Symantec has
 24 never denied a document request by Korean authorities on the basis that documents were located
 25 outside of Korea.” Chapman Decl., ECF No. 21, ¶ 9.

26 Korean police can compel testimony or the production of documents in the United States to
 27 assist the Korean criminal investigation only by making a formal request to the United States via the
 28 Mutual Legal Assistance Treaty (“MLAT”) between the United States and South Korea. Son Decl.,

ECF No. 4, ¶ 5, Ex. A (Treaty on Mutual Legal Assistance in Criminal Matters, Nov. 23, 1993, U.S.-S. Korea, S. Treaty Doc. No. 104-1 (1995) (entered into force May 23, 1997)). As far as Symantec's lawyer knows, the Korean authorities have not submitted an MLAT request. Hwang Decl., ECF No. 20-3, ¶¶ 8-9.

C. The Current State of the Korean Investigation

O2CNI says that the Korean Public Prosecutor's Office is continuing to collect documents and evidence pursuant to its investigative powers in preparation for filing a formal indictment against the former O2CNI employees, Mr. Owyang, Mr. Chapman, and the Symantec entities. Shin Decl., ECF No. 5, ¶ 31; Son Decl., ECF No. 4, ¶ 4. Symantec counters that the Korean Public Prosecutor's Office (a) is nearing the conclusion of its investigation, (b) has denied requests to issue arrest or detention warrants due to lack of evidence that the materials were trade secrets (especially regarding whether they were maintained confidentially) or that there was a conspiracy, and (c) has issued no indictments and will render a decision on whether to seek an indictment in the near future. Hwang Decl., ECF No. 20-3, ¶¶ 4, 5, 11.

III. THE SUBPOENAS

The subpoenas to Symantec Corporation and Mr. Owyang are identical, contain 17 document requests, and notice depositions on the document requests. *See* Application, Exs. A & B, ECF No. 1, at 4-33. Symantec objects on many grounds including relevance, overbreadth, confidentiality, proprietary information, privilege, work product, undue burden, and cumulative of discovery already provided in Korea. *See* Opposition, ECF No. 20 at 18-21; Chapman Decl., ECF No. 21 at 4-7 & Exs. A and B, ECF Nos. 20-1 & 20-2 (Symantec's objections). Symantec argues, for example, that O2CNI has not tailored its discovery to the subject matter of the Korean criminal investigation and instead is undertaking a "vast and unjustified fishing expedition." Opposition, ECF No. 20 at 18. It says that the documents contain commercially-sensitive documents regarding business and competitive strategies, pricing and revenues, research and development, production, and technical specifications and architecture for its products world-wide, all of which have substantial commercial value. *Id.* Once this highly-sensitive information (and actual trade secrets) are taken out of the United States, a protective order is ineffective. *Id.* at 21. O2CNI disagrees, asserts that its requests

1 are narrowly tailored, says that Symantec offers no basis for concluding that the documents are
2 duplicative of those Symantec provided voluntarily to the Korean police, challenges Mr. Chapman's
3 assertions about undue burden as "speculation and guesswork," and offers a protective order to be
4 sure that the trade secrets remain confidential and are used only in legal proceedings. Reply, ECF
5 No. 26 at 7-9, 17-20.

6 The following chart captures the document requests and the specific disagreements about them.
7 The chart has six areas: (1) summary of the requests (taken from the subpoenas themselves); (2)
8 O2CNI's initial justifications (taken from the initial Shin Declaration); (3) Symantec's objections to
9 the justifications (taken from its written objections and the Chapman Declaration); (4) O2CNI's
10 responses to Symantec's objections (taken from the Shin Reply Declaration); (5) Symantec's replies
11 to O2CNI's responses (taken from the Stone Declaration); and (6) O2CNI's replies to those replies
12 (taken from O2CNI's attorney's written objections to the Stone declaration). *See* Application, Exs.
13 A & B, ECF 1 at 4-33 (subpoenas); Shin Decl., ECF No. 5; Opposition, Exs. A and B, ECF Nos. 20-
14 1 and 20-2 (objections to requests); Chapman Decl., ECF No. 21 at 4-7; Shin Reply Declaration,
15 ECF No. 28 at 2-18; Stone Decl., ECF No. 35-1; O2CNI's Objections to Stone Declaration, ECF
16 No. 39. Not all document requests resulted in six back-and-forths. Some, for example, had only
17 four. The chart captures in summary fashion all back-and-forths for each request. The summaries
18 are intended to be descriptive and are not exhaustive.

Request #	Summary of Requests; O2CNI's Justifications; Symantec's Objections; O2CNI's Responses; Symantec's Replies; and O2CNI's Replies
1	<p>Summary: All policies and procedures regarding document retention or destruction (informal or formal) from January 1, 2007 to the present.</p> <p>O2CNI: Seeks information re Symantec's document retention and Symantec's and Mr. Owyang's alleged non-responsiveness to the Korean authorities' investigative demands. Relevant to determining whether Symantec and Mr. Owyang have concealed their wrongdoing by purging relevant documents or transferring information to servers outside of Korea.</p> <p>Symantec: Encompasses confidential, privileged, and work-product information; seeks documents outside the relevant time period and is cumulative to documents produced in the Korean criminal investigation. Overbroad. Opposition, Exs. A, B, ECF Nos. 20-1 & 20-2.</p> <p>O2CNI: The purpose is for policies and procedures that would apply to documents that are (or but for their destruction would have been) relevant to the foreign proceedings in that they would show whether Symantec tried to conceal the wrongdoing by purging its files or transferring information to servers outside of Korea. The 2007 time period is because that is the point when O2CNI developed and began providing services for products enumerated in request 2 that Symantec provisioned by using O2CNI's trade secrets. Shin Reply Decl., ECF No. 28, ¶¶ 4-7.</p>

2

Summary: Corporate structure and personnel (including organizational charts) from January 1, 2007 for 21 divisions (such as Telesales, Norton Startup Services, and Virus and Software Solution).

O2CNI: Identification of Symantec employees with knowledge of wrongful disclosures and appropriation of O2CNI's trade secrets in order to compete unfairly.

Symantec: Seeks corporate structure and personnel for 20 products and services over a six-year period since 2007 and over 4 years before the alleged misappropriation. Not confined to products in Japan or Korea or to its employees there; involves thousands of employees world-wide; Symantec has no central repository so would need to search individual files of employees who worked on the numerous product lines, which would take hundreds of hours by employees and counsel. Opposition, ECF No. 20 at 21; Opposition, Exs. A, B, ECF Nos. 20-1 & 20-2; Chapman Decl., ECF No. 20, ¶ 11.

O2CNI: This is meant to be the typical organization chart for high-level employees who are knowledgeable about products that O2CNI believes are infringing, not a list of thousands of employees who ever worked for the 21 enumerated departments. The 2007 time period is because that is when O2CNI developed and began providing services for products that Symantec provisioned by using O2CNI's trade secrets. O2CNI agreed to exclude three products (Norton PC Checkup, Norton PC Plus, and Norton Plus) but the information for the remaining 18 products and services is "highly relevant" to the foreign proceedings. As to two departments, O2CNI has documents that show that O2CNI disclosed trade secrets to Chapman and Owyang and that they both discussed their communications with O2CNI employees with other members of their department. As to the remaining 16 products and services, 12 were developed or originally provided by O2CNI in Korea or Japan, and "on information and belief" Symantec is providing these same services using O2CNI's trade secrets. Shin Reply Decl, ECF No. 28, ¶¶ 8-17.

Symantec: O2CNI identifies 13 products and services (out of the 16 in the last paragraph) that it says that Symantec provides using O2CNI's trade secrets, and it says that O2CNI developed or originally provided these in Japan or Korea. They are virus and spyware removal, remote installation, PC troubleshooting, and other PC technical support services. Symantec (and not O2CNI) developed these services here and around the world before it first contracted with O2CNI in April 2007 to provide call center support for customers in Korea and Japan. Stone Decl., ECF No. 35-1, ¶¶ 2, 6-18.

O2CNI: The Stone declaration is an impermissible attempt to argue the merits. *See* O2CNI's Objections to Stone Declaration, ECF No. 39.

1 2 3 4 5 6 7	3	<p>Summary: Personnel information (citizenship, home and work addresses, and employment status and history) and job descriptions for Mr. Owyang and Mr. Chapman from January 2009 to the present.</p> <p>O2CNI: This is to determine the whereabouts of Mr. Owyang (in case he tries to evade service) and Mr. Chapman (to obtain discovery from him individually).</p> <p>Symantec: Privacy, cumulative, already produced in Korean Investigation. Opposition, Exs. A, B, ECF Nos. 20-1 & 20-2.</p> <p>O2CNI: If they try to evade service or is elsewhere, O2CNI needs to find them or be able get discovery in that jurisdiction. Shin Reply Decl., ECF No. 28, ¶¶ 18-21.</p>
8 9 10 11 12 13	4	<p>Summary: Comprehensive documents about the hiring of the former employees, their employment evaluations, discussions regarding the benefits of hiring them, documents kept by HR, and their employment status.</p> <p>O2CNI: Relevant to wrongful solicitation and retention of the former employees by Symantec in order to compete unfairly with O2CNI.</p> <p>Symantec: Same as 3. Also many of documents are actually held by Symantec Pacific Pte Ltd in Singapore, not in the United States. Opposition, Exs. A, B, ECF Nos. 20-1 & 20-2; Chapman Decl., ECF No. 21, ¶ 12.</p> <p>O2CNI: Same as initial justification. Shin Reply Decl., ECF No. 28, ¶¶ 22-23.</p>
14 15 16 17 18 19 20 21 22 23	5	<p>Summary: “All documents and things written, created, produced, sent, or delivered by each of the Former O2CNI employees from January 2009 to the present.”</p> <p>O2CNI: Communications with former employees and the transmission of O2CNI’s confidential information and trade secrets to Symantec relating to the ROI Project, Project Red, and IR people, which are words that O2NCI discovered in other communications regarding disclosure of its confidential information and trade secrets</p> <p>Symantec: This broad request over five and a half years is not limited to time, and the employees began working only in 2011. They previously provided support at O2CNI for Symantec customers and thus frequently communicated with Symantec about routine customer support matters. Chapman Decl. ¶ 13.</p> <p>O2CNI: O2CNI employees destroyed their records before they left, so O2CNI cannot tell exactly what happened and when, and Symantec appears to be the only source. O2CNI thinks it is reasonable to start two and one-half years before their former employees joined Symantec. Shin Reply Decl., ECF No. 28, ¶¶ 24-28.</p>

1 2 3 4 5 6 7 8 9 10	6	<p>Summary: All documents regarding “Project Red” including business requirements documents, financial assessments, forecasts, analyses, studies, plans, reports, e-mails, memoranda, evaluations, projections, expectations, presentations or discussions.</p> <p>O2CNI: Same as 5.</p> <p>Symantec: This covers 27 individuals, including in-house counsel and senior executives, and does not define Project Red or provide any justification. Project Red predated the hiring of O2CNI’s former employees and concerned Symantec’s plans for customer support for countries other than Japan and Korea. Documents contain confidential and proprietary information about Symantec’s customer support services, and this has commercial value to competitors. Chapman Decl., ECF No. 20, ¶¶ 14-15.</p> <p>O2CNI: “Project Red” is Symantec’s term for taking over remote technical services being provided by O2CNI in Japan and Korea. Shin Reply Decl., ECF No. 28, ¶¶ 29-33.</p>
11 12 13 14 15	7	<p>Summary: All documents that include the term “Project Red” including those that also include 11 specified terms (BRD, Business Requirements Documents, BRR Log, Meeting Minutes, Action Tracker, Core Team, Korea Team, Core Staff, Coreteam, Q&A, and QnA).</p> <p>O2CNI: Same as 5.</p> <p>Symantec: Same as 6.</p> <p>O2CNI: Same as 6.</p>
16 17 18 19 20 21	8	<p>Summary: All documents and things that have ever been uploaded to network folders or document repositories concerning Project Red including those uploaded to https://www.symdocs.symad.symantec.com/sites/Project-Red and subfolders thereof.</p> <p>O2CNI: Same as 5.</p> <p>Symantec: Same as 6.</p> <p>O2CNI: Same as 6.</p>
22 23 24 25 26 27 28	9	<p>Summary: “All documents and things that have ever been received, sent, created, revised, or kept by” 27 specific employees concerning Project Red.</p> <p>O2CNI: Same as 5.</p> <p>Symantec: Same as 6. This also would require hundreds of hours of review of emails and computers of the 27 employees for the term “Project Red.” <i>See</i> Chapman Decl., ECF No. 20, ¶ 15.</p> <p>O2CNI: Same as 6.</p>

1 2 3 4 5 6 7 8	10	<p>Summary: All documents or things concerning ROI project.</p> <p>O2CNI: Same as 5.</p> <p>Symantec: No limitation as to time, employee, or subject matter. “ROI” (means return on investment) and “project” are generic and often-used terms at Symantec. A search would result in millions of results on diverse and unrelated matters. Also likely contain confidential and proprietary information with commercial value to competitors. Chapman Decl., ECF No. 20, ¶ 16.</p> <p>O2CNI: This is a term used by Symantec and former O2CNI employees to describe a plan the O2CNI employees proposed to leave O2CNI and either (1) work for Symantec and provide the same services or (2) form an independent company to provide services for Symantec. Shin Reply Decl., ECF No. 28, ¶¶ 39-43.</p>
9 10 11 12 13 14 15 16 17 18 19	11	<p>Summary: All documents and things concerning “IR People” from January 1, 2011 to the present, including “documents Symantec has ever sent or received from IR People, all State of Work documents exchanged with IR People, documents concerning Symantec’s retention of IR people, decision to retain IR People, and the amount of Symantec’s consulting fee payments to IR people, and invoices Symantec received from IR People.</p> <p>O2CNI: Same as 5.</p> <p>Symantec: Trade secrets, competitive harm, cumulative to that produced. Opposition, Exs. A, B, ECF Nos. 20-1 & 20-2.</p> <p>O2CNI: IR People is owned by a Mr. Sung-Ho Cho, a close acquaintance of Young-Oh Yeom (one of the former O2CNI employees). Cho arranged a meeting with Owyang and Yeom in October 2011 while Yeom was an O2CNI employee to discuss setting up Symantec’s call center to provide the same services provided by O2CNI. Cho created the IR entity in December 2011, and thereafter, Symantec paid IR People to provide services for the Korean call center such as recruiting, training, set up of IT equipment, and testing. This was the vehicle used to channel trade secrets even before October 2011. Shin Reply Decl, ECF No. 28, ¶¶ 44-47.</p>

12

Summary: Documents and things to show the technical specifications and architectures of the CRM, VOIP, and CTI systems used to provide 18 identified services and all products and services out of Symantec's Korea call center from January 1, 2009 to the present.

O2CNI: Relevant to Symantec's use of O2CNI's trade secrets and confidential information.

Symantec: Seeks information regarding Symantec's own products and services that O2CNI once supported, which – pursuant to the parties' own contracts – is Symantec's own confidential information. The documents show the technical design of the customer relationship management ("CRM") system, phone systems, and CTI (computer-telephone integration) used by Symantec globally to provide customer support for its products around the world since 2009. CRM describes broad categories of systems and technologies relating to managing interactions with customers, including VOIP (voice communications over the Internet) and CTI (technology allowing computer-telephone integration). This would require a search for all call centers across the world. The information is confidential and proprietary, and disclosure would put Symantec at a commercial disadvantage. Opposition, ECF No. 20; Chapman Decl., ECF No. 20, ¶ 17. Disclosing information would provide O2CNI detailed insight into Symantec's internal business methods, processes, products, and services, all of which are not publicly available. Chapman Decl., ECF No. 20, ¶¶ 7, 17, 18. Involves over 20 Symantec products and services over four and a half years, and O2CNI provides no justification as to how these sweeping requests – pertaining to the support of Symantec products using widely-used technologies – are relevant to any claimed trade secret of O2CNI.

O2CNI: Same as in 2. O2CNI will exclude 3 products, but 13 of the remaining products were developed and or provided by O2CNI in Korea and Japan. Three more involved provisioning by Symantec outside of Korea and Japan using O2CNI's CRM, VoIP, or CTI-related trade secrets. The last item involves products and services provided by Symantec in its Korean call center by some or all of the former O2CNI employees using O2CNI's trade secrets. Shin Reply Decl., ECF No. 28 at 16.

Symantec: Same as in 2. Symantec, not O2CNI, developed the 13 products and services.

O2CNI: The Stone declaration is an impermissible attempt to argue the merits. *See* O2CNI's Objections to Stone Declaration, ECF No. 39.

1 2 3 4 5 6 7 8 9 10 11 12	13	<p>Summary: Documents showing the contents of the technical support materials used by call center employees to provide the same services specified in request 12 from January 1, 2009 to the present.</p> <p>O2CNI: Same as 12.</p> <p>Symantec: Same as 12. Seeks (a) confidential and proprietary information describing Symantec's own products and services that it provides to customer support personnel and (b) documents about Symantec's plans to market its own products and services. This is not publicly-available information, and its disclosure would be of substantial value to Symantec's competitors and harm Symantec. Chapman Decl., ECF No. 20, ¶ 18.</p> <p>O2CNI: Same as 12. Seeks information regarding Symantec's misappropriation of trade secrets relating to its provisioning of telephonic technical support services. Shin Reply Decl., ECF No. 28, ¶¶ 57-58.</p> <p>Symantec: Same as in 2. Symantec, not O2CNI, developed the 13 products and services.</p> <p>O2CNI: The Stone declaration is an impermissible attempt to argue the merits. <i>See</i> O2CNI's Objections to Stone Declaration, ECF No. 39.</p>
13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28	14	<p>Summary: For the same services in requests 12 and 13, all documents and things relating to planning, researching, developing, improving, commercializing, and launching the services from January 1, 2009 to the present.</p> <p>O2CNI: Same as 13.</p> <p>Symantec: Same as 12.</p> <p>O2CNI: Seeks information relevant to Symantec's misappropriation of trade secrets in providing the enumerated products and services. Shin Reply Decl., ECF No. 28, ¶¶ 59-60.</p> <p>Symantec: Same as in 2. Symantec, not O2CNI, developed the 13 products and services.</p> <p>O2CNI: The Stone declaration is an impermissible attempt to argue the merits. <i>See</i> O2CNI's Objections to Stone Declaration, ECF No. 39.</p>

1 2 3 4 5 6 7 8 9 10 11 12 13 14	15	<p>Summary: All documents and things relating to the CRM of Salesforce.com.</p> <p>O2CNI: Same as 12. Also, no temporal limitation. Opposition, ECF No. 20 at 21.</p> <p>Symantec: This encompasses Symantec’s customer service relationship for all products and services worldwide, including enterprise products that O2CNI never supported. The request for Symantec’s use of customer relationship management (“CRM”) without limitation for time or manner is a request for all data ever entered by every Symantec employee into Symantec’s customer relationship database (used by Symantec company-wide for CRM for all products and services). This covers terabytes of information of highly confidential data about Symantec’s business and customer relationships, and would likely reveal customers’ confidential and sensitive information about customers’ internal operations and security. Opposition, ECF No. 20 at 18-19; Chapman Decl., ECF No. 20, ¶ 19.</p> <p>O2CNI: Symantec uses Salesforce.com to deploy CRM and CTI systems in its products and services as part of Project Red. O2CNI has alleged that Symantec misappropriated its O2CNI’s CRM-related trade secrets, so information about Salesforce.com is relevant. O2CNI will limit this to the products and services in requests 12 through 14 (and will exclude the three products we excluded there). Shin Reply Decl., ECF No. 28, ¶¶ 62-65.</p> <p>Symantec: Same as 2. Symantec, not O2CNI, developed the 13 products and services.</p> <p>O2CNI: The Stone declaration is an impermissible attempt to argue the merits. <i>See</i> O2CNI’s Objections to Stone Declaration, ECF No. 39.</p>
15 16 17 18 19 20 21 22 23 24 25 26 27	16	<p>Summary: Documents to show the revenue, profits, and losses from January 1, 2009 to the present for the same services broken out by country.</p> <p>O2CNI: Same as 12.</p> <p>Symantec: Contains highly-sensitive information relating to the revenues, profits, and losses for over 20 Symantec products and services broken out by country around the world. Symantec publicly reports its consolidated financial information, but this country-by-country information is confidential, commercially sensitive, and is of competitive value to Symantec’s customers if publicly known. Still objectionable even if limited to Korea and Japan, but its irrelevance is demonstrated by the fact that it seeks information for products and services outside of Japan and Korea. Opposition, ECF No. 20 at 18-19; Chapman Decl., ECF No. 20, ¶ 20.</p> <p>O2CNI: O2CNI needs this information to quantify its damages. 2009 is appropriate time period for reasons discussed in 12. Shin Reply Decl., ECF No. 28, ¶¶ 66-67.</p> <p>Symantec: Same as 2. Symantec, not O2CNI, developed the 13 products and services.</p> <p>O2CNI: The Stone declaration is an impermissible attempt to argue the merits. <i>See</i> O2CNI’s Objections to Stone Declaration, ECF No. 39.</p>

17	<p>Summary: All document and things concerning the Korean Criminal Investigation, including documents about Symantec's and Mr. Owyang's decision to decline to respond to investigative demands by the Korean authorities and any investigation commissioned by Symantec.</p> <p>O2CNI: Same as 1.</p> <p>Symantec: The only responsive documents are all confidential communications between Symantec employees and legal counsel. Chapman Declaration, ECF No. 20, ¶ 21.</p> <p>O2CNI: The purpose is to get information regarding Symantec's and Owyang's refusal to participate in the Korean proceedings and their efforts to obstruct those proceedings by destroying or concealing documents. Shin Reply Decl., ECF No. 28, ¶ 68.</p>
----	--

ANALYSIS

28 U.S.C. § 1782(a) authorizes foreign tribunals, litigants, and other "interested persons" to obtain discovery in the United States for use in foreign proceedings. More specifically,

The district court of the district in which a person resides or is found may order him to give his testimony or statement or to produce a document or other thing for use in a proceeding in a foreign or international tribunal, including criminal investigations conducted before formal accusation. The order may be made pursuant to a letter rogatory issued, or request made, by a foreign or international tribunal or upon the application of any interested person and may direct that the testimony or statement be given, or the document or other thing be produced, before a person appointed by the court.

28 U.S.C. § 1782(a). An "interested person" is one who "possesses a reasonable interest in obtaining [judicial] assistance" and includes a complainant who "triggers" an investigation by a state investigative body or a litigant in a foreign action. *See Intel Corp. v. Advanced Micro Devices, Inc.*, 542 U.S. 241, 256 (2004). "A person may not be compelled to give his testimony or to produce a document or other thing in violation of any applicable legal privilege." 28 U.S.C. § 1782(a); *see In re Microsoft Corp.*, 428 F. Supp. 2d 188, 196 (S.D.N.Y. 2006) (quashing section 1782 subpoenas seeking work product).

A section 1782 application for discovery does not require that a formal proceeding in the foreign jurisdiction be currently pending or even imminent. *Id.* at 258-59. Instead, all that is necessary is that a "dispositive ruling" by the foreign adjudicative body is "within reasonable contemplation." *Id.* at 259 (holding that discovery was proper under § 1782 even though the applicant's complaint

1 against the opposing party was only in the investigative stage). An *ex parte* application is an
 2 acceptable method for seeking discovery pursuant to § 1782. See *In re Letters Rogatory from Tokyo*
 3 *Dist., Tokyo, Japan*, 539 F.2d 1216, 1219 (9th Cir. 1976) (holding that the subpoenaed parties may
 4 raise objections and exercise their due process rights by bringing motions to quash the subpoenas).

5 A district court has wide discretion to grant or deny discovery under § 1782. *Intel*, 542 U.S. at
 6 260-61, 264-65. “[A] district court is not required to grant a § 1782(a) discovery application simply
 7 because it has the authority to do so.” *Intel*, 542 U.S. at 264; see *id.* at 247 (“We caution, however,
 8 that § 1782(a) authorizes, but does not require, a federal district court to provide judicial assistance
 9 to foreign or international tribunals or to ‘interested person[s]’ in proceedings abroad.”).

10 When considering an application for discovery pursuant to 28 U.S.C. § 1782, the court considers
 11 first whether it has the statutory authority to grant the request and then whether it should exercise its
 12 discretion to do so. *Lazaridis v. Int’l Centre for Missing and Exploited Children, Inc.*, 760 F. Supp.
 13 2d 109, 112 (D.D.C. 2011) (citations omitted).

14 **I. THE STATUTORY REQUIREMENTS ARE MET**

15 The parties agree, and the court held previously, that the statutory factors are met for the court to
 16 issue an order pursuant to 28 U.S.C. § 1782 are met. Memo, ECF No. 2 at 15-19, Opposition, ECF
 17 No. 20 at 10; 8/15/13 Order, ECF No. 41 at 9. Symantec Corporation and Mr. Owyang are both in
 18 this district, the discovery sought is “for use” in the Korean criminal proceedings, and O2CNI is an
 19 “interested person” in those proceedings. The court thus considers how the *Intel* factors impact the
 20 court’s discretionary decision about whether to allow discovery under 28 U.S.C. § 1782.

21 **II. THE DISCRETIONARY DECISION**

22 A district court’s discretion is to be exercised in view of the twin aims of section 1782: (1)
 23 providing efficient assistance to participants in international litigation and (2) encouraging foreign
 24 countries by example to provide similar assistance to our courts. See *Schmitz v. Bernstein Liebhard*
 25 *& Lifshitz, LLP*, 376 F.3d 79, 84 (2d Cir. 2004). There is no requirement that the party seeking
 26 discovery establish that the information sought would be discoverable under the governing law in
 27 the foreign proceeding or that United States law would allow discovery in an analogous domestic
 28 proceeding. See *Intel*, 542 U.S. at 247, 261-63.

1 In exercising its discretion to grant or deny the discovery application, the court considers the
 2 following factors: (1) whether the “person from whom discovery is sought is a participant in the
 3 foreign proceeding”; (2) “the nature of the foreign tribunal, the character of the proceedings
 4 underway abroad, and the receptivity of the foreign government or the court or agency abroad to
 5 U.S. federal court judicial assistance”; (3) whether the request “conceals an attempt to circumvent
 6 foreign proof-gathering restrictions or other policies of a foreign country or the United States”; and
 7 (4) whether the request is “unduly intrusive or burdensome.” *See id.* at 264-65. The court also may
 8 consider whether the section 1782 request is a “‘fishing expedition’ or a vehicle for harassment,” *In*
 9 *re Request for Assistance from Ministry of Legal Affairs of Trinidad & Tobago*, 848 F.2d 1151, 1156
 10 (11th Cir. 1988), abrogated in other part by *Intel*, 542 U.S. at 259; *see Intel*, 542 U.S. at 266;
 11 *Lazaridis*, 760 F. Supp. 2d at 115 n.5; and whether the complaint in the foreign jurisdiction is merely
 12 pretextual, *see Intel*, 542 U.S. at 266.

13 The first *Intel* factor is whether respondents Symantec Corporation and Mr. Owyang are
 14 “participant[s] in the [Korean] foreign proceeding.” *Intel*, 542 U.S. at 264. If they are, then “the
 15 need for § 1782(a) aid generally is not as apparent as it ordinarily is when evidence is sought from a
 16 nonparticipant in the matter arising abroad” because “[a] foreign tribunal has jurisdiction over those
 17 appearing before it, and can itself order them to produce evidence.” *Id.* (citations omitted). By
 18 contrast, “nonparticipants in the foreign proceeding may be outside the foreign tribunal’s
 19 jurisdictional reach; hence, their evidence, available in the United States, may be unobtainable
 20 absent § 1782(a) aid.” *Id.* (citation omitted).

21 Here, the parties do not dispute that (1) Symantec, Mr. Owyang, and Mr. Chapman are named as
 22 criminal suspects in O2CNI’s criminal complaint to the Korean authorities and (2) they have
 23 declined to travel to Korea to give voluntary interviews. *See supra* p. 6. The parties disagree about
 24 whether Symantec has provided documents voluntarily. Symantec says that it has never declined a
 25 document request from Korean authorities on the basis that documents were located outside of
 26 Korea. *See* Chapman Decl., ECF No. 21, ¶ 9. O2CNI counters that only subsidiary Symantec Korea
 27 has provided documents. *See* Reply, ECF No. 26 at 10 (citing Hwang Decl., ECF No. 20-3, ¶ 8). It
 28 adds that “Symantec Corp., Owyang, and Chapman have *refused* to participate and never provided

1 the testimony or documents sought by Korean authorities.” Reply, ECF No. 26 at 10; *see* Park
 2 Decl., ECF No. 31, ¶¶ 3-4 (a Korean police inspector told O2CNI’s Vice President that on three
 3 occasions, he faxed formal requests to appear to the CEO of Symantec Corporation, Mr. Owyang,
 4 and Mr. Chapman).⁶

5 This factual context shows that Symantec Corporation and Mr. Owyang are not participants in
 6 the criminal proceedings. Respondents nonetheless argue that by naming them as criminal suspects
 7 in its complaint, O2CI rendered them “participants,” but they provides no authority for that
 8 conclusion, and they do not dispute that they refused to respond to the requests to appear. *See*
 9 Opposition, ECF No. 20 at 11.

10 But the conclusion that Respondents are not participants does not end the inquiry under the first
 11 *Intel* factor or tip this factor automatically in O2CNI’s favor, especially given that there are no
 12 defendants in preliminary criminal proceedings, only suspects. *See Lazaridus*, 760 F. Supp. 2d at
 13 114. Also, the *Intel* factors involve overlapping considerations, are considered collectively by the
 14 court in exercising its discretion, and are not stand-alone categorical imperatives. In reaching the
 15 conclusion that discovery is not appropriate on this record, the court considered the following.

16 First, part of the factor one inquiry is that status as a participant means that the foreign tribunal
 17 can order discovery from the participant, and status as a non-participant means that the foreign
 18 tribunal cannot. *See Intel*, 542 U.S. at 264. At least as far as interviews or depositions are
 19 concerned, the authorities in Korea (just like U.S. authorities) apparently cannot compel interviews
 20 or depositions of criminal suspects (at least on topics that are self-incriminating). *See* Huang Decl.,
 21 ECF No. 20-3, ¶¶ 5-6; *see also* U.S. CONST. amend. V. Of course, when considering a section 1782
 22 application for discovery, the unavailability of testimonial discovery in Korea and in the United
 23 States is not dispositive because there is no requirement that the requesting party establish that the
 24 information is discoverable in the foreign proceeding or in an analogous proceeding here. *See Intel*,
 25 542 U.S. at 247, 262-63. Still, given the important procedural protections that a criminal suspect has
 26 here and in Korea, the context of a criminal investigation (under *Intel* factor two) informs a court’s

27
 28 ⁶ Whether a request to appear necessarily includes a separate request for documents is not
 clear from the record. It seems plausible that it does.

1 discretionary decision about whether to order discovery. This context weighs in favor of the court's
 2 discretionary decision on this record to deny testimonial discovery (at least to the extent that it is
 3 self-incriminating).⁷

4 Second, as to the production of documents, Respondents are not in Korea and apparently are not
 5 subject to that court's jurisdiction. Under factor one, that is the classic reason for document
 6 discovery and weighs in favor of discovery. Under factor two, the nature of the proceeding, a
 7 victim's request for documents – on its own and without any other context – is neutral (as the court
 8 held previously). *See* 8/15/13 Order, ECF No. 41 at 12-13.

9 One reason that a document request (standing alone) is neutral is that Korean authorities have
 10 used the MLAT process for criminal cases and are receptive to U.S. federal-court judicial assistance.
 11 *See id.* They presumably would be receptive to the discovery because they made requests to the
 12 Respondents themselves. Also, any reluctance to seek production in this case does not necessarily
 13 signal resistance to receipt of evidence. *See Intel*, 542 U.S. at 261-62.⁸ Moreover, there is no
 14 requirement that discovery in aid of a criminal case must be through an MLAT process. The
 15 existence of a formal process for criminal authorities to gain discovery through official channels

16
 17 ⁷ Under the MLAT, issues of immunity and privilege are for the requesting state's courts to
 18 decide. *Son Decl.*, Ex. A, ECF No. 4 at 24 (MLAT, Article 8(4)). That negotiated provision
 19 governs official requests for assistance that go through official channels and are vetted and approved
 20 by both the requesting state and the requested state (which on this side would be DOJ-OIA). That
 21 approach makes sense: the MLAT is a negotiated treaty for mutual legal assistance. But deference
 22 to a requesting state's procedures pursuant to a negotiated treaty does not translate into automatic
 23 deference to a requesting victim. An interested person who is not the requesting state might have
 24 entirely different motives than (for example) a requesting prosecutor. That is why, under *Intel*, the
 section 1782 inquiry involves the court's exercise of discretion and consideration of the scope,
 purpose, and context of a request by an interested person. The difference between interested persons
 and requesting states is also the reason that the court previously recognized the procedural
 safeguards inherent in an MLAT process when information is sought directly from the criminal
 suspect.

25 ⁸ As the Supreme Court explained, "[a] foreign nation may limit discovery within its domain
 26 for reasons peculiar to its own legal practices, culture, or traditions; such reasons do not necessarily
 27 signal objection to aid from United States federal courts. A foreign tribunal's reluctance to order
 28 production of materials present in the United States similarly may signal no resistance to the receipt
 of evidence gathered pursuant to § 1782(a)." *Intel*, 542 U.S. at 261-62 (internal and external
 citations omitted).

1 does not mean that victims cannot obtain discovery in aid of a foreign criminal investigation. The
 2 plain language of the statute permits it. A complainant who triggers a foreign civil investigation has
 3 a significant role in the process. *See Intel*, 542 U.S. at 256. A complainant's status as a victim in a
 4 criminal investigation does not alter that conclusion and might (depending on the case and the
 5 context of the complainant's request) enhance its interest. For that reason, courts have allowed
 6 discovery to victims in aid of the foreign investigation. *See Consorcio Minero S.A. v. Doe Run*
 7 *Resources Corp. and DR Acquisition Corp.*, No. 4:11-MC-583 (CEJ), 2011 WL 4550200, at *3
 8 (E.D. Mo. Sept. 30, 2011).⁹ Also, seeking documents does not alone constitute any evasion of
 9 foreign proof-gathering restrictions (*Intel* factor three).

10 Third, the facial neutrality of a document request does not mean that discovery in aid of a foreign
 11 criminal investigation is always neutral or that a victim/complainant's request necessarily is
 12 equivalent to a formal request from a foreign government. For example, courts exercise their
 13 discretion to deny discovery when a complainant's motives are not demonstrably to aid the criminal
 14 investigation and instead are a "fishing expedition." *See Lazaridis*, 760 F. Supp. 2d at 112; *see also*
 15 *supra* note 6 (describing the differences between requesting interested parties and requesting
 16 states).¹⁰

17 In *Lazaridis*, the applicant (Lazaridis) sought discovery from the International Centre for
 18 Missing and Exploited Children and the National Center for Missing and Exploited Children. *See*

20 ⁹ In *Consorcio Minero*, a mineral trading company (Cormin) asked for discovery from the
 21 U.S. corporations that were the former and current indirect parents of a Peruvian company called
 22 Doe Run Peru. *See* 2011 WL 4550200, at *1. Doe Run Peru allegedly owed Cormin \$29 million.
 23 *Id.* Doe Run Peru's direct parent was Doe Run Cayman, and Doe Run Cayman claimed that Doe
 24 Run Peru owed it \$156 million, which made it Doe Run Peru's largest creditor and gave it control
 25 over Doe Run's debts, including its debt to Cormin. *Id.* Cormin challenged whether part of the debt
 26 (\$139 million of the \$156 million) was an improper "insider" debt and sought discovery from the
 27 U.S. corporations for use in a Peruvian civil action about the validity of the Doe Run Cayman's
 28 purported debt and in two criminal cases, one initiated by Doe Run Peru against Cormin for libel
 and one initiated by Cormin against Doe Run Peru. *Id.*

¹⁰ The court did an exhaustive search for cases involving victim/complainants who seek
 discovery in aid of foreign investigations, and there are few section 1782 cases. That explains why
 most of the cases cited by the parties involve civil cases. This case-law context heightened the
 court's unease with O2CNI's broad document requests.

1 760 F. Supp. 2d at 111. He claimed to be an interested party in a pending Greek criminal
2 prosecution against the president of the National Center (and others) and in a “penal investigation”
3 of the same individuals, and he sought records from the respondent companies about allegedly false
4 advertisements that children were missing. *Id.* The court held that Lazaridis was an interested
5 person at least for the criminal investigation and that the court thus had the authority to permit
6 section 1782 discovery. *Id.* at 113-14.

7 As to the first factor, the court held that it weighed against discovery because the respondents
8 were necessarily participants in the Greek prosecution because the lead defendant was president of
9 the National Center. *Id.* at 114. The fact that they were not parties in the criminal investigation
10 “was inconsequential . . . because there are no defendants in an investigation, only suspects.” *Id.*

11 More relevant to this case, the court held that the nature of the case weighed against granting the
12 application. *Id.* at 114-15. Part of the reason for that conclusion was that Lazaridis’s “wide-ranging
13 request suggests that [he] is seeking information more for his general use than for use by the Greek
14 tribunals in their investigation or prosecution of specific criminal acts.” *Id.* at 115. The court noted
15 that Lazaridis had not credibly shown, for example, how the documents he asked for would aid the
16 Greek authorities in the criminal investigation of “falsely advertised” missing children. *Id.* at 115
17 n.5. The court observed that “[s]ection 1782 is not a device for a fishing expedition.” *Id.* The court
18 also said that the Greek prosecutor could obtain documents under the relevant MLAT, that the
19 respondents reasonably surmised that the Greek prosecutors and court did not need Lazaridis’s
20 assistance, and that “mere inaction” by the Greek authorities “does not transfer into their agreement
21 or consent.” *Id.* at 115.

22 Fourth, as in *Lazaridis*, O2CNI’s “wide-ranging” requests suggest that they are seeking the
23 information for their own use and not for use in the Korean criminal case. As in *Lazaridis*, it is the
24 nature of the request that weighs against granting the application. The court is not equating O2CNI
25 with Mr. Lazaridis. They are very different applicants, and the court understands that. But as in
26 *Lazaridis*, O2CNI has not shown how its broad requests would aid the Korean authorities, and their
27 extraordinary scope makes them appear so out of proportion to their utility in the criminal case that
28 it gives the court considerable pause as to O2CNI’s motives.

Trade secrets cases often are fraught with all sorts of emotional context, and the document requests and O2CNI's justifications and purported "narrowing" (summarized *supra* ¶. 10-18) suggest an attempt to get at every aspect of Symantec Corporation's business that remotely touches on O2CNI's call-center business. The Shin Reply Declaration (also captured in the chart) did not narrow the requests in any meaningful way. By contrast, useful discovery in a criminal (or a civil) trade secrets case starts with a forensic analysis about what happened so that the court has some confidence that there actually was a theft of trade secrets and that discovery can be targeted to that theft. Usually that involves identifying what trade secrets are at issue under California Civil Code § 2019.210.¹¹ That allows targeted and effective discovery that is appropriate, cost-effective, and not unduly burdensome. Usually a complainant can conduct an investigation on its own end to identify what was taken and during what time period. That is true even when – as here – there is an allegation that departing O2CNI deleted computer files. Files can be recovered and restored (and if they cannot, then the requesting party ought to say so and why). Here, for example, O2CNI alleged conclusorily that it recovered emails that "suggest" disclosure of confidential trade secrets, Shin Decl., ECF No. 5, ¶ 18, but it provided no specifics and provided only high-level allegations about its alleged trade secrets (a communications network allowing billing at Korean rates and a "knowledge" base), *see id.*, ¶¶ 11, 29. Often, counsel propose realistic approaches that are cost-effective and illuminate the forensic lay of the land. For example, one can identify files taken and use their hashes to run a broader script across computers. If there are specific emails that suggest transmission of trade secrets, then identifying them allows good lawyers – and good lawyers represent Symantec – to do their job.

This was not O2CNI's approach here. The court's concern about the enormously broad discovery was heightened by what it perceived as a tack-on of hypothetical civil litigation. *See* 8/15/13 Order, ECF No. 41 at 11-12. And the requests are not targeted toward a criminal

¹¹ The court understands that section 2019.210 does not apply here, but in trade-secrets cases in the Northern District, parties usually do not argue that it does not apply in federal court. The point here is that it provides a mechanism to frame the appropriate scope of discovery, including discovery in aid of a criminal case.

1 investigation and instead are broad-ranging inquiries by a former vendor into its competitor that are
2 beyond reasonable first-step discovery in any case. The court's conclusion was that the requests
3 were breathtaking in their scope and so broad as to be a fishing expedition.¹² Also, the court's view
4 was that at least the criminal investigation is not prejudiced because the MLAT process provides a
5 mechanism to aid the Korean prosecutors if they want it.

6 Another issue is that Symantec made strong arguments (including arguments that Symantec
7 developed a good portion of the products and services that O2CNI attacks as using its trade secrets).
8 *See supra* p. 16 (chart). It talked about how the requests implicate widely-used technologies for call
9 centers (such as VoIP and CTI). *See supra* p. 15 (chart). The requests were sweeping and involved
10 an enormous amount of commercially-sensitive information without any obvious relevance to a
11 criminal investigation. O2CNI challenged Symantec's arguments as "speculation and guesswork"
12 ungrounded in any factual basis, but its own justifications are equally so, and Symantec's
13 explanations are more obviously plausible given that this case implicates a call center. Put another
14 way, it is very easy understand Symantec's arguments, and O2CNI's justifications and so-called
15 narrowing provide no basis for understanding why the court should grant their broad requests.
16 Indeed, there is a basis for concluding that they are going after their competitor after their former
17 employees decamped and refused to sign non-compete and confidentiality agreements. O2CNI
18 attacks Symantec's arguments as impermissibly arguing the merits, but Symantec's arguments give
19 context to broad subpoenas that even on their own appear to be a fishing expedition. This is another
20 reason why actually alleging the trade secrets with some specificity might have given some record
21 for the court to conclude that O2CNI's requests were made in good faith and not to harass.

22 A final point is that the court's conclusion is only that discovery in aid of the Korean
23

24 ¹² The court appreciates that it did not use the words "fishing expedition" in the first order.
25 But as the tone of the hearing revealed, the court found the discovery requests so broad as to be
26 offensive in a request implicating a criminal case. It may be that O2CNI's joining of the
27 hypothetical Japanese civil proceedings to the criminal inquiry resulted in a broader request than it
28 might have made only in a criminal case. Nonetheless, on the record here, the court's concern was
that the requests were so broad here as to have (at best) tangential relevance to a restitution
determination in a criminal case and implicated privilege issues and burdens far beyond that
appropriate in any trade secrets case, regardless of the forum.

1 investigation is not appropriate “on this record.” The anchoring to “this record” is because the court
2 can see how one might draft an appropriately-targeted request in a trade secrets case such as this
3 one. Again, O2CNI did not do that. The court disagrees with O2CNI’s argument that the court
4 ought to tailor discovery, not deny it outright. *See* Motion for Relief, ECF No. 45 at 21. It was
5 O2CNI’s job to make appropriate requests, and it did not do so. Its overbroad requests in this case
6 provide no basis for the court to be able craft reasonable requests, and thus the court can deny the
7 application in full. *See In Re Apotex, Inc.*, No. 12-160, 2009 WL 618243, at *3 (S.D.N.Y. Mar. 9,
8 2009) (citations omitted).

9 CONCLUSION

10 For the foregoing reasons, on this record the court exercise its discretion and **DENIES** O2CNI’s
11 application for discovery. The court’s view is that this order does not foreclose O2CNI from
12 submitting a new application with appropriate requests tailored to the Korean criminal investigation.
13 This approach makes sense given a victim’s/complainant’s important interest in a criminal
14 investigation against a potential wrongdoer.

15 This disposes of ECF No. 1.

16 **IT IS SO ORDERED.**

17 Dated: October 29, 2013



18 LAUREL BEELER
United States Magistrate Judge